Format and topics for exam 2
Math 127

General information. Exam 1 will be a timed test of 75 minutes, covering Sections 3.5–3.6, 4.2, 5.3–5.6, and 6.1–6.4 of the class notes/text. More to the point, the exam will cover the portions of PS04–06 coming from Chs. 3–6 and the ideas contained therein. No books, notes, calculators, etc., are allowed.

As before, most of the exam will rely on understanding the problem sets and the definitions and theorems that lie behind them. If you can do all of the homework, and you know and understand all of the definitions and the statements of all of the theorems we've studied, you should be in good shape. You should not spend time learning proofs of theorems from the book, except the ones assigned on homework. On the other hand, you should defintely spend time learning the *statements* of the important theorems in the text.

Exam 2 will follows the same ground rules as Exam 1 did, and there will be the same possible types of questions: computations, proofs, explanations/problem solving, true/false/justify, and statements of definitions/theorems.

Definitions. The most important definitions and symbols we have covered are:

3.5	divides	common divisor
	greatest common divisor	associates
	up to associates	irreducible
	reducible	
4.2	binary operation	ring
	domain	inverse
	unit	field
	fraction	$\frac{a}{b}$
5.3	F^n	vector
	zero vector	scalar
	vector addition	scalar multiplication
	subspace	linear combination
	coefficients of a lin. comb.	trivial lin. comb.
	nontrivial lin. comb.	span (noun)
	span (verb)	spanning set
	linearly dependent	linear dependency
	linearly independent	basis
	dimension	coordnates
5.4	$n \times k$ matrix	matrix addition
	scalar multiplication	row-column product
	dot product	matrix-vector product
	matrix product	column space
	$\mathrm{Col}(A)$	nullspace
	$\mathrm{Null}(A)$	
5.5	linear equation	system of linear equations
	homogeneous linear system	matrix of a linear system
	REF	leading 1
	pivot column	RREF
	pivot variable	free variable
	elementary row operations	Gaussian reduction
	rank	nullity
5.6	maximal linearly independent set	
6.1	parity check code of length $n+1$	repetition code of length n

6.2	bit	bitstring of length n
	code	codeword
	binary linear code of length n	standard framework
	encoding	decoding
	correct	read
	generator matrix	parity check matrix
	syndrome	
6.3	Hamming 7-code	$\mathcal{H}_7$
	Hamming 8-code	$\mathcal{H}_8$
6.4	$[n, k, d]$ binary linear code	Hamming distance
	Hamming weight	Hamming path of length k
	metric	

Theorems, results, algorithms. The most important theorems, results, and algorithms we have covered are listed below. You should understand all of these results, and you should be able to state any theorem clearly and correctly. More precisely, you should be able to state any of the theorems, given a reasonable identification of the theorem (either its name or a vague description).

Sect. 3.5 Euclidean Algorithm for polynomials (Alg. 3.5.4). EA works (Thm. 3.5.6), common divisors divide GCD (Cor. 3.5.7). GCD unique up to associates (Cor. 3.5.9). Unique Factorization for Polynomials (Thm. 3.5.12).
Sect. 3.6 Bezout's Identity for polynomials (Thm. 3.6.1). Linear equations in $F[x]$ (Cor. 3.6.3).
Sect. 4.2 Zero factor property implies cancellation (Thm. 4.2.8). Fields are domains (Thm. 4.2.12). Fraction notation works (Thm. 4.2.14).
Sect. 5.3 Span is a subspace (Thm. 5.3.8); a basis gives unique coordinates (Thm. 5.3.15).
Sect. 5.4 Algebraic properties of matrix multiplication (Thm. 5.4.7). Nullspaces are subspaces (Thm. 5.4.9); columns are linearly independent if and only if nullspace is 0 (Thm. 5.4.10).
Sect. 5.5 Solving a homogeneous linear system in RREF (Alg. 5.5.3). RREF gives basis for nullspace (Thm. 5.5.5). Gaussian reduction (Alg. 5.5.7). Columns linearly independent if and only if all pivot (Cor. 5.5.10). Finding a basis for $\mathrm{Col}(A)$ (Thm. 5.5.12). Rank-nullity (Cor. 5.5.15).
Sect. 5.6 Comparison Theorem 5.6.2, Dimension Theorem 5.6.3, dim is min span/max linearly independent (Cor. 5.6.4). Maximal linear independent set is a basis (Thm. 5.6.6); bases always exist (Cor. 5.6.7). Subspace Size Theorem (Cor. 5.6.8).
Sect. 6.1 Majority logic for repetition code (6.1.3).
Sect. 6.3 Decoding $\mathcal{H}_7$ (Alg. 6.3.2); $\mathcal{H}_7$ corrects 1 error Thm. 6.3.4. $\mathcal{H}_8$ corrects 1 error, detects 2 (Thm. 6.3.6).
Sect. 6.4 Hamming distance is shortest Hamming path (Thm. 6.4.8), is translation invariant (Cor. 6.4.9), is a metric (Thm. 6.4.11). Nearest-neighbor error correction (Alg. 6.4.12). Nearest neighbor corrects $\lfloor (d-1)/2 \rfloor$ errors, detects $\lfloor d/2 \rfloor$ errors (Thm. 6.4.13).

Examples. You will also need to be familiar with the key properties of the main examples we have discussed. The most important examples we have seen are:

Sect. 3.5 Euclidean Algorithm (Exmp. 3.5.5).
Sect. 3.6 Euclidean Rewriting example (Exmp. 3.6.2).
Sect. 4.2 Rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $R[x]$, $\mathbb{Z}/(n)$. Fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/(p)$ (p prime).
Sect. 5.3 Bitstrings are elements of $\mathbb{F}_2^n$. Subspaces: F^n, zero subspace, subspace $\mathcal{C}$ from Sect. 5.1. Bases for F^n, zero subspace, subspace $\mathcal{C}$ from Sect. 5.1.
Sect. 5.4 Matrix-vector multiplication is linear combination of columns.
Sect. 5.5 Solving equations in RREF. Gaussian reduction. Analysis of subspace $\mathcal{C}$ from Sect. 5.1.
Sect. 5.6 Calculating: $\mathrm{Col}(A)$, $\mathrm{Null}(A)$, rank, nullity in various situations.
Sect. 6.1 Parity check code, repetition code.
Sect. 6.2 Parity check code by parity check matrix; repetition code from generator matrix.

Sect. 6.3 Encoding and decoding in $\mathcal{H}_7$.
Sect. 6.4 $[n, k, d]$ stats of: parity check code, repetition code, $\mathcal{H}_7$, $\mathcal{H}_8$. Hamming distance.

Other. You should have a working familiarity with techniques and strategies for proof and logic tips, to the extent that we have done proofs in the homework. You should also review how to prove that a set is closed under a given operation (Section 1.3.4).

Not on exam. Sections 4.1, 4.3, 5.1–5.2.

Good luck.